[0017]

Fig. 2 is a block diagram of a hardware mechanism constituting an IC card 100 of an embodiment of the present invention. The IC card 100 includes a CPU 210, an input/output interface (I/O) 220, a ROM 230, a RAM 250, and an EEPROM 240. The ROM 230 indicates a nonvolatile memory whose memory content is readable but not rewritable. The RAM 250 and the EEPROM 240 are memories whose memory content is readable and rewritable, and the RAM 250 indicates a volatile memory that loses the memory content when an electric supply to the IC card 100 is cut off while the EEPROM 240 indicates a nonvolatile memory that does not lose the memory content even when the electric supply to the IC card 100 is cut off.

[0018]

Fig. 1 is a block diagram of the IC card 100 of Fig. 2 in which each constituent for realizing the present invention is provided. A memory 110 indicates a storage area that is assigned in the RAM 250 or the EEPROM 240 of Fig. 2. Encryption/decryption program storage means 111 for storing encryption/decryption programs that encrypt data to be kept secret or decrypt the data thus encrypted is assigned in the memory 110.

[0019]

Further, data storage means 112 for storing data received by the IC card 100 or data to be processed in the IC card 100 is assigned to an area different from that of the encryption/decryption program storage means 111 in the memory 110.

[0020]

Each of the encryption/decryption programs stored in the

encryption/decryption program storage means 111 is managed by encryption/decryption program management data 113 (*corresponding to "encryption/decryption program administrating data" in the previous translation*). Fig. 9 is one example of the encryption/decryption program management data.

[0021]

In a case where a certain encryption/decryption program is selected in a process in the IC card 100, encryption/decryption program selecting means 120 refers to the encryption/decryption program management data 113, so that the designated encryption/decryption program is selected.

[0022]

In a case where a certain encryption/decryption program is registered in the encryption/decryption program storage means 111 or a certain encryption/decryption program that has been already registered in the encryption/decryption program storage means 111 is deleted, encryption/decryption program registering/deleting means 130, based on a result of the designated encryption/decryption program selected by the encryption/decryption program selecting means 120, (i) registers management data in the encryption/decryption program management data 113 provided in the encryption/decryption program storage means 111 and incorporates the designated encryption/decryption program in the memory 110, or (ii) deletes corresponding management data from the encryption/decryption program management data 113 and deletes corresponding encryption/decryption program from the memory 110.

[0023]

In a case where a certain encryption/decryption program is activated in the IC card 100, encryption/decryption program activation means 140 activates the designated

encryption/decryption program, based on a result of the designated encryption/decryption program selected by the encryption/decryption program selecting means 120, so that data to be encrypted, stored in data storage means 112, is encrypted or decrypted.

[0024]

In a case where, in the encryption/decryption program activation means 140, the encryption/decryption program management data 113 for the designated encryption/decryption program stores data of the encryption/decryption program itself requiring to be decrypted, encryption/decryption program encrypting/decrypting means 150 decrypts the designated encryption/decryption program, and the encryption/decryption program activation means 140 activates the designated encryption/decryption program thus decrypted.

[0025]

In a case where the IC card 100 receives data or an encryption/decryption program from an external information processing device or transmits data or an encryption/decryption program to an external information processing device, encryption/decryption program and data transmission/reception means 160 transmits data to or receives data from a communication line 101 by use of the input/output interface (I/O) 220.

[0026]

In the block diagram of Fig. 1, the encryption/decryption program selecting means 120, the encryption/decryption program registering/deleting means 130, the encryption/decryption program activation means 140, the encryption/decryption program encrypting/decrypting means 150, and the encryption/decryption program and data transmission/reception means 160 are provided in either one of

the ROM 230 and the EEPROM 240, each of which is a nonvolatile memory in the IC card 100.

[0027]

The following explanation deals with one example of encryption of data and transmission of the data thus encrypted by use of the IC card 100 of the embodiment illustrated in Figs. 1 and 2, with reference to Figs. 3 through 9.

[0028]

Fig. 3 illustrates a process of the encryption/decryption program and data transmission/reception means 160 for transmitting data to the communication line 101, or receiving data from the communication line 101, each by use of the input/output interface (I/O) 200 of the IC card 100. The process checks whether or not there is data to be transmitted or received by a determination process of S310 and S330, which allows data transmission/reception any time when the IC card 100 is in a running state.

[0029]

Fig. 8 illustrates a format of data to be transmitted or received. When there is received data, an S340 process is carried out for determining a data type included in a header section of the received data. The data type is set so as to have information for determining which of an encryption program, a decryption program, and data, the received data is. In a case where the received data is an encryption/decryption program, an S350 process is carried out such that an identifier of the encryption/decryption program is read out from the data to be received, and an S400 process is carried out for checking whether or not there is an encryption/decryption program corresponding to the designated identifier.

[0030]

Fig. 4 illustrates a flow of an encryption/decryption

program selecting process in S400. In the encryption/decryption program selecting process S400, an identifier identical with the identifier of the encryption/decryption program received is searched from the encryption/decryption program management data 113 that is set in the EEPROM 240 and the RAM 250. In a case where a corresponding identifier is found (S420), encryption/decryption program management data corresponding to the identifier is returned. Meanwhile, in a case where the corresponding identifier is not found, it is judged that the identifier is not registered, and an error code is set and returned to a call of the S400 process.

[0031]

The target encryption/decryption program management data 113 to be searched in the S400 process is in a format illustrated in Fig. 9. An identifier for identifying an encryption/decryption program is constituted by a card ID in which the encryption/decryption program is stored, and an encryption/decryption program number that is managed in the card. Management data of the encryption/decryption program is constituted by a storage address of an encryption program in the IC card 100, a storage address of a decryption program in the IC card 100, and a memory type (EEPROM or RAM) registered in the IC card 100. In a case where the encryption/decryption program itself requires to be decrypted before the registered encryption/decryption program is executed, the management data further includes an identifier of the encryption/decryption program, used for the decryption (in a column of decryption process).

[0032]

In the example of Fig. 9, when a card ID of an IC card 100 concerned is "C001", there are two types of

encryption/decryption program identifiers registered by the IC card 100 concerned: "C00101" and "C00102" (an identifier is represented such that a registration card ID is sequentially followed by No), and an encryption/decryption program whose identifier is "C00102" is encrypted by that of "C00101". Further an encryption/decryption program identifier "C02010" means that only management data of a decryption program that decrypts data at a time when the data is received from a card ID "020" is stored. Furthermore, an encryption/decryption program identifier "C00000" indicates an encryption/decryption program that is registered in the IC card 100 as a standard program so that the identifier "C00000" can be used commonly for all IC card. The encryption/decryption program identifiers "C00101" and "C03011" indicate that programs thereof are encrypted by that of "C00000" registered as a standard.